I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

Come Fly the (Unfriendly?) Skies: Negotiating Passenger Name Record Agreements Between the United States and European Union

Marjorie J. Yano*

Abstract: This note examines the progress of negotiations of Passenger Name Record ("PNR") Agreements between the United States and the European Union following the terrorist attacks of September 11, 2001. First, this note looks at the need for such information sharing between the U.S. and the EU and the original PNR Agreement signed in 2004. It then examines the implications of the European Court of Justice's annulment of the 2004 agreement, the interim agreement in 2006, and the subsequent agreement signed in 2007. In looking at each of these agreements, this note considers both the compromises that have been made in constructing these agreements as well as the tensions that still exist with regard to the international exchange of personal data. Finally, this note looks at how the Obama Administration may need to approach continued relations with the European Union with respect to PNR agreements.

I. 9/11 AND THE NEED FOR EU PNR DATA

Following the terrorist attacks of September 11, 2001, the United States government realized that there was a clear need for increased regulation of our nation's aviation system; in particular, there was a need for increased awareness of who had access to commercial aircraft and who was booking flights into and within the United States.[1] The

*Marjorie Yano is a J.D. candidate at The Ohio State University Moritz College of Law. She is concurrently pursuing a Master of Arts in Public Policy and Management from The Ohio State University John Glenn School of Public Affairs. She is a 2007 graduate of Amherst College with a B.A. in History and Political Science.

results of subsequent regulations and rules were obvious for travelers: more thorough inspections at airport security check-points across the country, increased baggage searches, and tighter restrictions on carry-on items.[2] These regulations changed the nature of air travel in a new, post-9/11 United States.[3] However, with all the obvious changes that were occurring in the wake of 9/11, there were equally important, but much less visible, changes occurring in United States law and foreign policy.

Incorporated into these less visible changes were new early-detection measures, intended to warn U.S. authorities of potentially dangerous travelers before they could cause any problems. In 2003, the Transportation Security Administration ("TSA") began screening domestic air travelers using the Computer-Assisted Passenger Pre-Screening System II program ("CAPPS II").[4] The program, which required passengers to provide personal information (such as full name, address, phone number, and date of birth) to the airline's computer reservation system, automatically conducted a full background check—giving the TSA information about the traveler's history, including a credit and banking history as well as a full criminal background check.[5] Not surprisingly, privacy groups within the United States decried CAPPS II as an invasion of privacy, but the program was defended by the Department of Transportation, which stated that the program "is being designed with the utmost concern for the individual privacy rights of American citizens."[6]

Since then, the scope of data collection has expanded, and the United States government has reached out across the Atlantic, to the European Union, in an effort to create a more comprehensive

---

[1] Monte R. Belger, Statement before the Committee on the Judiciary, Subcommittee on Technology, Terrorism, and Government Information, on Security Technology, United States Senate (Nov. 14, 2001) *available at* http://www.iwar.org.uk/comsec/resources/senate-biometrics/te111401st-belger.htm.

[2] *See, e.g.*, Transportation Security Administration Prohibited Items, http://www.tsa.gov/travelers/airtravel/prohibited/permitted-prohibited-items.shtm (last visited April 8, 2010).

[3] Paul Zielbauer & John Sullivan, *After the Attacks: Airport Security, FAA Announces Stricter Rules, Knives No Longer Allowed*, N.Y. TIMES, September 13, 2001, at A5.

[4] Roy Mark, *TSA Books Data Mining Program*, INTERNETNEWS.COM, March 4, 2003, http://www.internetnews.com/bus-news/article.php/2013781.

[5] *Id.*

[6] *Id.*

information basis for fighting terrorism in the skies. However, if it was difficult for the United States to face claims of privacy infringement solely under U.S. law, the situation that faced the Bush Administration in the negotiation of PNR Agreements with the EU was much more complicated. While international cooperation is vital to successfully combat global terrorist organizations, EU and U.S. law differ in some significant ways, and formulating an agreement—by which personal information about private citizens would be shared—has proved to be no easy task.[7]

II. ISSUES IN PROVIDING EU PNR DATA TO THE UNITED STATES

A. THE 1995 DIRECTIVE

The central concern within Europe is whether or not the PNR Agreements with the United States are consistent with EU privacy law. The most important piece of EU legislation in this area is Directive 95/46/EC of The European Parliament and of the Council of 24 October 1995 ("1995 Directive").[8]

The fundamental objective of this directive is for EU Member States to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[9] To achieve this goal, the 1995 Directive streamlines the laws of Member States to create an overarching framework of privacy laws and rights of EU citizens.[10]

Especially important to the debate over PNR Agreements is Article 8, which prohibits "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."[11] One problem in using PNR data to combat terrorism—or at least to keep an eye on individuals deemed to have

---

[7] EU Network of Independent Experts in Fundamental Rights (CFR-CDF), *The Balance Between Freedom and Security in the Response by the European Union and its Member States to the Terrorist Threats*, (March 31, 2003), 8 *available at* http://www.statewatch.org/news/2003/apr/CFR-CDF.ThemComment1.pdf.

[8] Council and Parliament Directive 95/46, 1995 O.J. (L 281) 31 (EC).

[9] *Id.*, ch. I, art. 1(1).

[10] *Id.* at (8).

[11] *Id.* at ch. II, sec. III, art. 8(1).

some suspicious speck on their records – is that the inclusion of racial or ethnic characteristics cuts against the prohibitions of Article 8. An independent committee of experts on fundamental rights in Europe released an opinion comment about the precarious balance between freedom and security in post-9/11 Europe, including how agreements with the United States may affect this balance.[12] In their discussion on the creation of "terrorism profiles," the group states:

> The inclusion of elements of identification such as "nationality," "education" or "family situation" in these profiles no doubt requires much greater care, particularly since there is an explicit relationship between these profiles and the policy on immigration. At the present stage, the procedures for the development of these terrorist profiles appear insufficient in terms of the accuracy and reliability of information, which is taken into account, notwithstanding its confidentiality, which cannot justify a total absence of control.[13]

Following 9/11, this provision took on particular relevance with respect to a general concern of racial or ethnic profiling by governments in attempts to combat and prevent terrorism.

Even in the most recent manifestation of the PNR Agreements, concerns about racial and ethnic profiling have not been completely allayed. The EU is right to worry: after 9/11, organizations such as the European Monitoring Center on Racism and Xenophobia noticed increased hostility towards, and abuse of, European Muslims.[14] Considering this trend in race and ethnic relations in Europe, as well as the dictates of the 1995 Directive, the European Union faced a difficult balance of ensuring adequate security and protection against future attacks, while still maintaining domestic peace and respecting the rights and privacy protections of individual citizens.

The concern of citizens, however, extends beyond the racism and xenophobia that emerged after 9/11. There are also questions about

---

[12] EU Network of Independent Experts in Fundamental Rights, *supra* note 7.

[13] *Id.* at 21.

[14] Anya Rudiger, Ph.D., Remarks at the St. Anthony-Princeton Conference – Muslims in Europe post 9/11 (April 26, 2002) *available at* http://www.sant.ox.ac.uk/ext/princeton/pap_rudiger.shtml.

what kind of sensitive personal information can be derived from the information given to airlines. As *The Register*, a British newspaper, reported, "[y]our travel records can reveal who you travel with and how often, how many beds you sleep in (and therefore your sexuality), who buys your travel tickets, and sometimes even, through the special meals you order, your medical condition or religion."[15] This is a difficult concern to address: while the EU may not process sensitive personal information about religion, ethnicity, or sex life, is it also prohibited from processing data from which this sensitive information can be derived? This concept continues to be an important element of the debate over PNR Agreements.

The transmission of PNR data also raises concerns under Article 25 of the 1995 Directive, which states that "[t]he Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."[16] The process by which an "adequate level of protection" is determined is based upon "all the circumstances surrounding a data transfer operation or set of data transfer operations" and is made in light of the laws and regulations in place in the third country.[17] It is only after the European Commission has determined that these adequate provisions are in place that the EU may engage in negotiations with countries outside the EU regarding the transfer of personal data.[18] If, however, an adequate level of protection is not found, then "Member States shall take measures necessary to prevent any transfer of data for the same type to the third country in question."[19] Thus, if the EU finds that the United States does not have adequate rules and regulations for the protection of personal data, then, based upon EU law, negotiations for PNR Agreements will stall completely because they would be prohibited by the 1995 Directive.

---

[15] Wendy M. Grossman, *The Great Passenger Name Record Sell Out*, THE REGISTER, August 12, 2007, http://www.theregister.co.uk/2007/08/12/pnr_sell_out/print.html.

[16] Directive 95/46, *supra* note 8, ch. IV, art. 25(1).

[17] *Id.* at (2).

[18] *Id.* at (5) – (6).

[19] *Id.* at (4).

B. THE ARTICLE 29 WORKING PARTY

The EU's Article 29 Working Party is central to the debate over privacy and how privacy can still be protected in an era where national security relies on the free flow of information between governments.[20] Following the attacks of September 11, 2001, the Working Party issued a series of opinions regarding "the latest state of the dialogue as regards commitments from the U.S. side on the conditions for processing of passenger PNR data by U.S. authorities."[21] In these opinions, the Working Party stated that while the exchange of PNR data is an important component in the global war on terrorism, safety from terrorism cannot be gained at the expense of personal liberties and privacy rights of individuals.[22] Citing a list of EU conventions, such as the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union, the Working Party argued that instead of racing headlong into PNR Agreements, "limitations on the fundamental rights and freedoms regarding the data protection principles governing the processing of personal data in the European Union should only take place if necessary in a democratic society for the protection of public interest."[23]

Consistently, the Working Party has been a voice of caution in negotiations over PNR Agreements. Specifically, it expressed concern over the lack of specificity in provisions of early PNR Agreements,[24] and consistently worked to ensure that the immediacy of the terrorism threat did not cause individual privacy rights to be forgotten in negotiations.

---

[20] Established in the 95 Directive, the Working Party is comprised of "a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission." The responsibilities of the Working Party include examining national measures adopted under the Directive to ensure uniformity of the laws of the Member States, and issuing opinions regarding the level of adequate protection of other EU legislation which would affect the rights of individuals with regard to the processing of personal information. *Id.* at Art. 29(2), Art. 30(1).

[21] Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), 10019/04/EN, WP 87, 29 January 2004, at 2.

[22] *Id.* at 3.

[23] *Id.*

[24] *See, e.g., id.* at 6 (vagueness of phrase "other serious crimes").

III. AGREEMENTS AND CONTROVERSY

A. THE 2004 AGREEMENT

In May 2004, the United States Department of Homeland Security ("DHS") and the European Union signed an international agreement ("2004 Agreement") which required "air carriers to provide U.S. Customs and Border Protection ("CBP") with access to passenger name records for purposes of screening individuals travelling to and from the United States."[25] Under the 2004 Agreement, this data was to be exchanged to "the extent it [was] collected and retained in the air carrier's automated reservation/departure control systems"[26] and would be used to screen individuals before their departure to or from the United States.[27] In the context of the 2004 Agreement, PNR data is defined as "a record of each passenger's travel requirements which contains all information necessary to enable reservations be processed and controlled by the booking and participating airlines."[28]

Under the 2004 Agreement, thirty-four data elements were requested by CBP from air carriers.[29] However, while the amount of

---

[25] Privacy Office, Department of Homeland Security, A Report Concerning Passenger Name Record Information Derived from Flights Between the U.S. and European Union, 18 December 2008, at 6-7.

[26] European Parliament v. Commission of the European Communities, Judgment of the Court (Grand Chamber), 30 May 2006, at 26 (citing *Undertakings of the Department of Homeland Security Bureau of Customs and Border Patrol (CBP)*, annexed to Commission Decision 2004/535, 2004 O.J. (L 235) 11).

[27] Privacy Office, *supra* note 25, at 7.

[28] Commission Decision 2004/535, 2004 O.J. (L 235) 11, at (4).

Under the Agreement, a "booking airline" is "an airline with which the passenger made his original reservations or with which additional reservations were made after the commitment of the journey." A "participating airline" means "any airline on which the booking airline has requested space, on one or more of its flights, to be held for a passenger."

[29] These data elements include: PNR record locator code, date of reservation, date(s) of intended travel, name, other names on PNR, address, all forms of payment information, billing address, contact phone numbers, all travel itinerary for specific PNR, frequent flyer information (limited to miles flown and address(es)), travel agency, travel agent, code share PNR information, travel status of passenger, split/divided PNR information, email address, ticketing field information, general remarks, ticket number, seat number, date of ticket issuance, no show history, bag tag numbers, go show information, OSI information, SSI/SSR information, received from information, all changes to the PNR, number of

data provided by the airlines to CBP was extensive, the use of PNR data by the United States was expressly limited in the 2004 Agreement. As the European Commission noted in its examination of the privacy protections in place under the 2004 Agreement, PNR data are used by CBP strictly for purpose of preventing and combating: 1. terrorism and related crimes; 2. flight from warrants or custody for the crimes above. Use of PNR data for these purposes permitted CBP to focus its resources on high-risk concerns, thereby facilitating and safeguarding bona fide travel."[30] The 2004 Agreement included numerous other restrictions on the transfer of PNR data between CBP and other United States government agencies. In particular, the 2004 Agreement stated that "CBP will judiciously exercise its discretion to transfer PNR data for the stated purposes."[31]

In exercising this discretion, CBP was required to first determine if the use for which transfer was required would be consistent with the stated purposes of the 2004 Agreement. If so, then CBP would determine whether the party to which the information would be transferred had a valid reason for pursuing enforcement of the purposes of the PNR—that is, whether the party is "responsible for preventing, investigating, or prosecuting the violations of, or enforcing or implementing, a statute or regulation related to that purpose."[32]

Another important aspect of the 2004 Agreement was that it provided rules about the storage of PNR data. Under the 2004 Agreement, CBP would permit access to PNR data for seven days, after which time, access to such data would be placed on a more restricted status for three and a half years.[33] After that time, any data that had not been accessed during the three and a half year period would be destroyed, while that which had been accessed would be transferred to a "deleted record file" to be held for eight years before destruction.[34] The length of time that the United States would retain

---

travelers on the PNR, seat information, one-way tickets, any collected APIS (Advanced Passenger Information System) information, and ATFQ (Automatic Ticketing Fare Quote) fields. Andreas Busch, *From Safe Harbrour to the Rough Sea? Privacy Disputes Across the Atlantic*, 3 SCRIPT-ED 304, 312 (June 2006).

[30] Commission Decision 2004/535, Annex, 2004 O.J. (L 235) 11, 15.

[31] *See* European Parliament v. Council of the European Union, *supra* note 26, at 26.

[32] *Id.*

[33] Commission Decision 2004/535, Annex, 2004 O.J. (L 235) 11, 17.

[34] *Id.*

PNR data later proved to be an important part of re-negotiation discussions, as Europeans were skeptical about the need for U.S. officials to keep unused (or little used) PNR data for such a long time.

B. 2004 ADEQUACY DETERMINATION

An important prerequisite for any PNR Agreement between the United States and EU is a determination by the European Union that the U.S. agencies receiving PNR data maintain adequate levels of protection over this information. This requirement is set out in Article 25 of the 1995 Directive and, in May 2004, The Commission of the European Communities announced its finding of adequacy with respect to the U.S. CBP.[35]

There are several points that seem to be central to the Commission's decision to permit PNR data transfers to the United States—and which also serve as the foundation of later disputes over the legality of subsequent PNR Agreements. First, because of the personal, and potentially sensitive, nature of the data subject to transfer, it was important that there be only one recipient of the information (to control the data as much as possible to prevent unnecessary dissemination). In this case, "the data transfers concerned involve specific controllers, namely airlines operating flights between the Community and the United States, and only one recipient in the United States, namely the CBP."[36] Limited transfer among U.S. government agencies was contemplated by the Commission, however, the legality of these transfers required that the U.S. have good reason to transfer PNR data outside CBP before such a transfer could be completed.[37] An important exception to the permissible transfer provisions is any public disclosures under the Freedom of Information Act ("FOIA")—in fact, the Commission explicitly stated that "no other foreign, federal, State or local agency has direct electronic access to PNR data through CBP databases. CBP will refuse public disclosure of PNR, by virtue of exemptions from the relevant provisions of FOIA."[38] Thus, tight control and limited access

---

[35] *See id.*

[36] *Id.* at (9).

[37] *Id.* at (11)-(13). The Commission cited Department of Homeland Security regulations and rules that would set forth the parameters of transfers within the U.S. government. *See* Undertakings of the Department of Homeland Security Bureau of Customs and Border Patrol of 11 May 2004.

[38] *Id.* at (20).

to PNR data by agencies or persons outside the CBP formed a crucial element to the Adequacy Decision of 2004.

Other important elements were transparency and the rights of access and ratification by the data subject.[39] The Adequacy Decision states that "the data subject may request a copy of PNR data and rectification of inaccurate data."[40] The foundation of the right to access and ratification stems from the 1995 Directive, which contains several sections relating to the data subject's right to access and challenge of that data.[41] Subject to certain limited exceptions, data subjects must receive notice about the identity of the data controller, purposes for processing the data, and any further information, including any recipients of the data and any rights to correction of inaccurate data.[42]

Thus, even while the Commission of the European Communities did find that the United States maintains an adequate level of protection for PNR data – and therefore that PNR Agreements are permissible under EU law – the terms and requirements of the handling of this data are important and would set the stage for later disputes over provisions of PNR Agreements.

C. 2006 EU PARLIAMENT CHALLENGE AS TO LEGAL BASIS OF THE 2004 AGREEMENT

The most significant challenge to PNR Agreements came in the form of a 2006 lawsuit, brought by the European Parliament to annul both the 2004 PNR Agreement between the EU and United States, and the Commission of the European Communities' Adequacy Decision.[43] In seeking to annul the Adequacy Decision, the European Parliament advanced "pleas for annulment, alleging, respectively, *ultra vires* action, breach of the fundamental principles of the [1995]

---

[39] *Id.* at (17)-(19).

[40] *Id.* at (19).

[41] *See generally* Council and Parliament Directive 95/46, *supra* note 8, at sections IV – VII.

[42] *See, e.g., id.* at section IV, art. 10.

[43] *See* European Parliament v. Commission of the European Communities, *supra* note 26, at (1).

Directive, breach of fundamental rights and breach of the principle of proportionality."[44]

The Parliament argued that the adequacy decision was inappropriate because elements of the 1995 Directive were not complied with—particularly Article 3(2) of that Directive. Article 3(2) stipulates that an exception exists with respect to the general prohibition on the electronic processing of personal data if the data is processed "in the course of an activity that falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defense, State security . . . and the activities of the State in areas of criminal law."[45]

The Parliament argued that the activities required under the 2004 Agreement *are* within the scope of Community law.[46] On the other hand, the Commission (which promulgated the Decision of Adequacy) disagreed, and drew a distinction between the private airline carriers collecting the information, and public authorities acting outside the scope of Community law. The key to this argument was that "Article 3(2) of the Directive refers to the activities of *public authorities* which fall outside the scope of Community law," while the Decision of Adequacy contemplated the transmission of PNR data by *private airline carriers*, which fall *within* the scope of Community law.[47]

Parliament's argument to annul the 2004 Agreement was based on two primary arguments: "the incorrect choice of Article 95 EC as the legal basis for the [2004 Agreement]" and the breach of "Article 8 of the [European Convention for the Protection of Human Rights], the principle of proportionality, the requirement to state reasons and the principle of cooperation in good faith."[48]

With respect to the incorrect legal basis for the 2004 Agreement, the Parliament argued that the 1995 Directive was improper because the decision "does not have as its objective and subject-matter the establishment and functioning of the internal market by contributing to the removal of obstacles to the freedom to provide services and it

---

[44] *Id.* at (50).

[45] *See* Council and Parliament Directive 95/46, *supra* note 8, art. 3(2).

[46] *See* European Parliament v. Commission on the European Communities, *supra* note 26, at (53).

[47] *Id.* at (53) (emphasis added).

[48] *Id.* at (62).

does not contain provisions designed to achieve such an objective."[49] Essentially, the Parliament argued that, because the exchange of PNR data is a matter of law enforcement and internal security, the power to make this kind of agreement does not rest with the centralized European Union in Brussels, but rather, with the individual European states.[50]

The European Convention on Human Rights ("ECHR") provided another important basis for the Parliament's arguments against the 2004 Agreement. Article 8 provides: "(1) Everyone has the right to respect for his private and family life, his home and his correspondence; (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[51]

Specifically, the Parliament argued that the 2004 Agreement and the Adequacy Decision violated provisions of necessity and proportionality contained within the ECHR.[52] Data retention by the government, in particular, came under fire as a violation of Article 8. As Privacy International, an organization devoted to the protection of personal privacy, noted: "The indiscriminate collection of traffic data

---

[49] *Id.* at (62-63).

[50] Stewart A. Baker & Nathan Alexander Sales, Homeland Security, Information Policy, and the Transatlantic Alliance (March 17, 2009). George Mason Law & Economics Research Paper No. 09-20, 11, *available at* SSRN: http://ssrn.com/abstract=1361943. The court notes that while the EU adopted the 2004 Agreement under its "First Pillar" powers of trade, travel, and other economic issues relating to the common European market, in fact, the agreement was not designed for economic purposes. Rather, its focus is security and law-enforcement. Therefore, the EU lacked authority to enter the agreement, because law-enforcement is not one of the powers given to the EU under European law. *See id.* at 11. *See also* Henriette Tielemans, et. al. The Transfer of Airline Passenger Data to the U.S.: An Analysis of the ECJ Decision, BNA International World Data Protection Report (June 2006), at 4, *available at* http://www.cov.com/files/Publication/8aa81e95-460a-4d30-a901-28b14757ec00/Presentation/PublicationAttachment/37f11b14-ff49-4e95-a5ce-2ee016f94329/oid23778.pdf (noting that with respect to "third pillar" law enforcement power, the Parliament's role is limited to non-binding resolutions and Member States often must unanimously consent to text of any resolution).

[51] European Convention on Human Rights, November 4, 1950, Art. 8 *available at* http://www.hri.org/docs/ECHR50.html.

[52] Tielemans, et. al. *supra* note 50, at 4.

offends a core principle of the rule of law: that citizens should have notice of the circumstances in which the State may conduct surveillance, so that they can regulate their behavior to avoid unwanted intrusions."[53] Concurrent with this requirement is the law that any interference into the private lives of individuals cannot be disproportionate, and any interference that is disproportionate is invalid because it "cannot be said to be necessary in a democratic society."[54] Thus, Parliament argued that, considering the rule of proportionality, the data processing and retention authorized by the 2004 Agreement is in violation of Article 8 of the ECHR.

D. 2006 EUROPEAN COURT OF JUSTICE DECISION

In May 2006, the Court of Justice of the European Communities ("ECJ") handed down an opinion that annulled both the 2004 Agreement and the Adequacy Decision on which it was premised.[55] Although the court decision was significant because it opened the door for future negotiations on the exchange of information between the U.S. and EU, the court's decision was less relevant to privacy law than it might seem at first glance; rather than focusing on the privacy concerns raised by Parliament, the decision was based on jurisdictional issues.

The case was in fact two separate cases that had been consolidated by the court for consideration. In the first part of the consolidated case, the court considered the legality of the Decision of Adequacy. In finding that the Decision was invalid, the court focused on the fact that the Decision violated Article 3(2) of the 1995 Directive. Article 3(2) is significant because it excludes from the Directive's scope "the processing of personal data in the course of an activity which falls outside the scope of Community law, . . . and in any case processing operations concerning public security, defense, State security and the activates of the State in areas of criminal law."[56] The purpose of PNR

---

[53] Privacy International, Memorandum of Laws Concerning the Legality of Data Retention with Regard to the Rights Guaranteed by the European Convention on Human Rights, October 10, 2003, 3, *available at* http://www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf.

[54] *Id.*

[55] *See* European Parliament v. Council of the European Union, *supra* note 26, at (61) and (70).

[56] *Id.* at (54).

data transfers to CBP is defined under U.S. law as "preventing and combating terrorism and related crimes, other serious crimes, including organized [sic] crime, that are transnational in nature, and flight from warrants or custody for those crimes."[57] Because of the law enforcement nature of the PNR transfers, the court concluded that "the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of criminal law."[58]

The court disagreed with the Commission's argument that, because the PNR data is collected by private operators for commercial purposes, it is not covered by Article 3(2) of the Directive. Instead, the court held that the transfer of this kind of data, in the manner contemplated when the Decision of Adequacy was made, does relate to public security and is thus outside the scope of Community law and subject to Article 3(2) of the Directive. The court then concluded that "the decision of adequacy must consequently be annulled."[59]

In annulling the 2004 Agreement, the court relied on its holding on the issue of the Decision of Adequacy finding that, because the 2004 Agreement "relates to the same transfer of data as the decision on adequacy and therefore to data processing operations" that are beyond the EU's authority under the Directive, the 2004 Agreement must also be annulled.[60]

E. INTERIM AGREEMENT

Apart from nullifying both the 2004 Agreement and the Decision of Adequacy on which it was based, the ECJ decision was also significant because it preserved the applicability of the Decision of Adequacy until September 30, 2006.[61] In deciding to extend the life of the Decision of Adequacy (and thereby allow for the continuance of the 2004 Agreement, or other manifestations of PNR Agreements), the court cited a need for "legal certainty and in order to protect persons concerned"—presumably to protect European citizens from whatever might happen if, after the ECJ decision, CBP was relieved of

---

[57] *Id.* at (55).

[58] *Id.* at (56).

[59] *Id.* at (58)-(61).

[60] *Id.* at (68).

[61] *Id.* at (73)-(74).

all obligations for the protection of PNR data already in the U.S.'s possession.[62]

In October 2006, the United States and European Union reached an Interim Agreement which would expire once a new, permanent agreement was reached (but no later than July 31, 2007).[63]

The content of the Interim Agreement was largely similar to the 2004 Agreement: the U.S. would "continue to process PNR data received and treat data subjects concerned by such processing in accordance with undertakings given in 2004."[64] The transfer of PNR data also remained the same as under the 2004 Agreement and the EU retained responsibility for ensuring that "air carriers operating passenger flights in foreign air transportation to or from the U.S. process PNR data contained in their automated reservation systems as required by the U.S. administration."[65]

There are several significant ways in which the Interim Agreement differed from the 2004 Agreement. First, the Agreement stated that the U.S. will not "pull" information from airline databases, but rather, the information will be "pushed."[66] This provision was arguably a victory for the European Union—the Article 29 Working Party had previously stated, in a 2004 report, that the push method of data transfer was superior to the previously used pull method.[67] As the Article 29 Working Party wrote: "It is a matter of general data protection principle that recipients should only be given data they actually need. In the 'pull' method . . . recipients are given all data. It is then their duty to filter out and use only the data for which they

---

[62] *Id.* at (73).

[63] Agreement on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security, U.S.-EU, Oct. 19, 2006, 2006 O.J. (L 298) 29, 30.

[64] Council of the European Union, *Council Adopts Decision On Signature of Agreement with the United States On the Continued Use of PNR Data*, EGOVMONITOR, October 17, 2006, http://www.egovmonitor.com/node/8116

[65] *Id.*

[66] *New EU-US Interim Deal on Passenger Name Record*, EDRI-GRAM, Number 4.19, October 11, 2006, http://www.edri.org/edrigram/number4.19/pnr.

[67] Article 29 Data Protection Working Party, "Push-Pull Factsheet," March 21, 2007, *available at* http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/pull-push_factsheet_/pull-push_factsheet_en.pdf, 2.

have authorisation [sic] under an agreement."[68] In contrast, under the push system, the airlines would be responsible for giving CBP the data covered by the Agreement.[69] This was significant because it did not require the EU to relinquish control of any data not covered by the Agreement.

Additionally, the Interim Agreement contained some negotiated victories for the U.S., including more allowances for transfers of PNR data between U.S. government agencies. Under the new agreement, "PNR data will be available also to several US counter-terrorism agencies, if they have comparable standards of data protection with the EU."[70] This expansion of data sharing within the U.S. was a departure from the 2004 Agreement and the subject of debate as the EU resisted any potentially risky or unnecessary dissemination of personal data.

F. NEGOTIATING THE 2007 AGREEMENT

As negotiations for the 2007 Agreement proceeded during the spring and early summer of 2007, two opponents to the proposed Agreements emerged and voiced strong opinions about privacy issues.

In February 2007, the Article 29 Working Party issued an opinion on the transfer of PNR data to U.S. authorities,[71] which focused on providing notice to passengers that data about them was being recorded, transferred, processed, and stored. As the Working Party noted, "according to the Directive, the obligation to inform data subjects is placed on the data controller."[72] Because in the end both the EU and U.S. would control personal information, it was necessary, in the view of the Working Party, for the Agreement to articulate a notification system by which data subjects would be alerted to the fact that their information was being collected, stored, and transferred. The Working Party believed that the airlines, their travel agents, or reservation systems should be the mechanism by which individuals

---

[68] *Id.*

[69] *Id.*

[70] *New EU-US Interim Deal on Passenger Name Record, supra* note 66.

[71] Opinion 2/2007 on Information to Passengers About Transfer of PNR Data to US Authorities, XXXX/07/EN, WP 132, 15 February 2007.

[72] *Id.* at 4.

are notified.[73] The principle behind this notice requirement was a "guarantee of fair processing in respect of the data subject," and was established by Articles 10 and 11 of the 1995 Directive, meaning that it carried significant weight for consideration.[74]

The European Parliament also lodged its own concerns about the proposed 2007 Agreement. In a resolution adopted in July 2007, the Parliament criticized the proposal as failing to meet its second objective of helping prevent and combat terrorism and international crime.[75] Parliament contended that the reason this objective could not be met with the proposal under consideration was that the proposal was "substantively flawed in terms of legal certainty, data protection and legal redress for EU citizens, in particular as a result of open and vague definitions and multiple possibilities for exceptions."[76] Instead, Parliament stated that "adequate protection of private and civil liberties of individual citizens and data quality controls are necessary if the sharing of data and information is to be a valuable and reliable tool in the fight against terrorism."[77] The language and tone of this resolution is important to recognize—Parliament was in agreement that information sharing is an integral part to the war against terrorism and international crime, however, it also recognized that it is simultaneously important to establish these channels of information sharing in ways that are protective of privacy rights.

The media also intervened in the discussion by publishing numerous stories on both sides of the Atlantic Ocean about the negotiations and upcoming PNR Agreement. On the British side of the discussion, the media was consistently concerned with what it saw as a "complete handover of the rights of people travelling to the United States."[78] As many news outlets saw it, the problem was not only that PNR data would be exchanged for the purpose of combating

---

[73] *Id.* at 2.

[74] *Id.* at 5.

[75] European Parliament Resolution of July 12, 2007 on the PNR Agreement with the United States of America, http://www.statewatch.org/news/2007/jul/ep-pnr-resolution-jul-07.pdf.

[76] *Id.* at (C).

[77] *Id.* at (E).

[78] David Millward, *US 'License to Snoop' on British Air Travellers*, TELEGRAPH.CO.UK, January 2, 2007, *available at* http://www.telegraph.co.uk/news/uknews/1538286/US-licence-to-snoop-on-British-air-travellers.html.

terrorism, but that the same information could be used when dealing with other serious (although, as of yet, not well defined) crimes.[79] This fear that personal information would be used inappropriately was at the forefront of European minds in the months leading up to a new PNR Agreement.

Another concern articulated by the British media was that of reciprocity of information exchanges. As *The Telegraph* (a British newspaper) stated, "Washington promised to 'encourage' U.S. airlines to make similar information available to EU governments—rather than compel them to do so."[80] The potential one-sided nature of future PNR Agreements was concerning for Europeans who would have rather seen a more *quid pro quo* approach to information sharing.

On the American side, the media's reaction to ongoing negotiations was less concerned and more conciliatory—noting various opportunities for compromise on PNR data exchanges. One article, quoting then-chief privacy officer of the DHS, Hugo Teufel, III, was optimistic that "there will very likely be increased privacy protections with respect to PNR data" in future Agreements, including "a decrease, perhaps even a significant decrease, in the amount of time [the passenger data] is retained."[81]

Thus, in the days and months leading up to the expiration of the Interim Agreement, it was clear that both sides had unrelenting concerns over privacy and security that would need to be addressed before a successful PNR Agreement could be reached.

G. 2007 AGREEMENT

In late July 2007, U.S. and European Union signed the 2007 PNR Agreement ("2007 Agreement"); this Agreement continued the mission of preventing and combating terrorism and transnational crime through mutual sharing of information and transfer of PNR data by air carriers to the U.S. Department of Homeland Security.[82]

---

[79] *Id.*

[80] *Id.*

[81] James Niccolai, *Compromise Possible in U.S.-E.U. Passenger Data Dispute*, CIO.COM, June 14, 2007, *available at* http://www.cio.com/article/print/119500

[82] Agreement between the United States of America and the European Union on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), *available at* http://www.dhs.gov/xlibrary/assets/pnr-2007agreement-usversion.pdf. In 2003, CBP

Coming on the heels of the Interim Agreement, one of the significant provisions of the 2007 Agreement was that it provided for DHS to "immediately transition to a push system for the transmission of data by such air carriers no later than January 1, 2008 for all such air carriers that have implemented such a system that complies with DHS's technical requirements."[83]

The 2007 Agreement also includes a provision for the periodical review of the implementation of the Agreement, both by the U.S. and the EU to ensure "the effective operation and privacy protection of their systems."[84] However, this emphasis on cooperation is limited, and it is relatively unclear from the terms of the Agreement exactly how stringent privacy measures must be—especially those taken by the United States. The 2007 Agreement does state that "DHS shall process PNR data received and treat data subjects concerned by such processing in accordance with applicable U.S. laws, constitutional requirements, and without unlawful discrimination, in particular on the basis of nationality and country of residence."[85] However, to the extent that these standards are different from standards within the EU, it is unclear whether the concerns voiced by the Article 29 Working Party, European Parliament, or the EU media have really been fully alleviated.

The significant and more detailed portion of the 2007 Agreement is not contained within the signed Agreement itself, but consists of two letters exchanged between Michael Chertoff, the U.S. Secretary of Homeland Security and Luis Amado, the President of the Council of the European Union.[86] The first letter articulates "the policies which DHS applies to PNR data derived from flights between the U.S. and European Union (EU PNR) under U.S. law."[87]

---

was moved from the Department of the Treasury to the newly-created Department of Homeland Security, as such, the 2007 PNR Agreement was negotiated to allow transfer of data from the EU to DHS, rather than only to CBP. *See generally* The U.S. Dept. of Homeland Security, "History: Who Became Part of the Department?" http://www.dhs.gov/xabout/history/editorial_0133.shtm (last visited April 8, 2010).

[83] 2007 PNR Agreement, *supra* note 82, at 4.

[84] *Id.* at 5.

[85] *Id.*

[86] Agreement on the Processing and Transfer of Passenger Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), U.S.-EU, Aug. 4, 2007, 2007 O.J. (L 204) 18.

[87] *Id.*

Significantly, the data requested by the United States under the 2007 Agreement was limited to only nineteen pieces of data.[88] Additionally, because the transfer and processing of sensitive personal data (such as that related to racial or ethnic origin, religious beliefs, or sexual orientation) was such a contentious issue, the handling of this information is addressed directly in the 2007 Agreement. As stated in the U.S. letter to the EU, to the extent that this kind of sensitive information reaches the U.S. through the transfer process, "DHS employs an automated system which filters those sensitive PNR codes and terms and does not use this information," and it is then deleted from the U.S. system.[89]

The United States also addressed Europe's concerns about access and redress. In its letter accompanying the 2007 Agreement, the DHS explicitly stated that it "maintains a system accessible by individuals, regardless of their nationality or country of residence, for providing redress to persons seeking information about or correction of PNR."[90] The U.S. also extended the protections of the U.S. Privacy Act and U.S. Freedom of Information Act over PNR data and subjects.[91] This means that although the U.S. does have some room for the public release of PNR information, it can only do so to the extent that such release is not prohibited by the Privacy Act. FOIA also provides

---

[88] *Id.* at 21-22. The newly requested pieces of information are: PNR record locator code; date of reservation/issue of ticket; date(s) of intended travel; name(s); available frequent flier and benefit information (*i.e.*, free tickets, upgrades, etc.); other names on PNR, including number of travelers on PNR; all available contact information (including originator information); all available payment/billing information (not including other transaction details linked to a credit card or account and not connected to the travel transaction); travel itinerary for specific PNR; travel agency/travel agent; code share information; split/divided information; travel status of passenger (including confirmations and check-in status); ticketing information, including ticket number, one-way tickets and Automated Ticket Fare Quote; all baggage information; seat information, including seat number; general remarks including OSI, SSI and SSR information; any collected APIs information; all historical changes to the PNR listed in numbers 1-18.

[89] *Id.* There are several narrow exceptions where sensitive data is not deleted by the U.S. once it has been identified. These include situations where "the life of a data subject or of others could be imperiled or seriously impaired." In these situations, DHS may retain sensitive data for up to 30 days, but will provide notice to the European Commission about such situations. *Id.*

[90] *Id.* at 23.

[91] *Id.*

another avenue by which PNR subjects may access their PNR data to check for accuracy.[92]

However, perhaps most significantly, not only were measures for access and redress included in the 2007 Agreement, but so were means for enforcement of these provisions. Under the new agreement, "[a]dministrative, civil, and criminal enforcement measures are available under U.S. law for violations of U.S. privacy rules and unauthorized disclosure of U.S. records."[93] So, the 2007 Agreement not only resolved concerns about privacy, security, access, and correction, but it also addressed the issue of enforcement.

Another contentious issue that arose under the 2004 Agreement was the length of time the U.S. would retain PNR data once it had been received. The 2007 Agreement stipulates that EU PNR data will remain in "active analytical database" for seven years, at which time it will be moved to "dormant, non-operational status," where it remains for an additional eight years.[94] This is a longer time than was provided for under the 2004 Agreement; however, concerns about the longer holding period may have been allayed in Europe by the increased opportunities for access and correction of PNR data.

H. EU REACTION TO 2007 AGREEMENT

Despite reports and discussions over privacy concerns in the months leading up to the 2007 Agreement, the European media's reaction to the 2007 Agreement was one of suspicion, mistrust, and general concern. *The Register* called the 2007 Agreement "The Great Passenger Name Record Sell Out" and claimed that, despite assurances to the contrary, sensitive data was not adequately protected under the Agreement and that passenger access provisions were not being thoroughly enforced.[95]

Another issue was the reduction of data fields requested—from thirty-five to nineteen. While at first glance this appeared to be a victory for Europeans – limiting the amount of data transferred to the United States – critics in Europe argued the opposite. As one

---

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] Wendy M. Grossman, *The Great Passenger Name Record Sell Out*, THE REGISTER, Aug. 12, 2007, *available at* http://www.theregister.co.uk/2007/08/12/pnr_sell_out/print.html.

commentator argued: "what the Americans and Europeans cunningly did is dupe the entire population by taking the list of 34, dropping two, and then taking less lines on the page. They merged items on one line."[96]

The provision outlining the acceptable uses of PNR data was criticized in Europe as being too vague. As one member of European Parliament stated in June 2007: "The PNR deal is simply bad. The purposes for which the personal data can be used are not sufficiently defined. Furthermore, data are being used not only for investigations but also for profiling and data mining (automated computer system) that makes profiles of individuals based on collected data."[97]

But the 2007 Agreement did not just spark a reaction in Europe—American media outlets also picked up on anxieties over the new PNR data exchange arrangement. Under the 2007 Agreement, if and when Europe ever implemented a PNR data processing system, the United States would be required to reciprocate arrangements made under the 2007 Agreement and provide the EU with data about American citizens traveling abroad.[98] In November 2007, *The Washington Post* carried an article about the implementation of this reciprocity provision, stating that, for the first time, American travelers' personal data would be exported to all EU states by airline carriers flying to Europe.[99] Criticisms of the proposal came from both sides of the Atlantic, primarily from civil libertarians and liberal politicians (who also generally opposed the 2007 Agreement). These critics expressed concern that there was still insufficient "evidence of how effective the use of these data are in the fight against terrorists."[100]

Of particular concerns for Americans was the possibility of the EU using algorithms on PNR data to create risk assessments. As James Harrison, an attorney with the Identity Project, noted: "Congress forbids the U.S. from conducting algorithms on passenger data

---

[96] *Id.*

[97] *EU-US Data-Sharing Deals Renew Privacy Concerns*," EURACTIV.COM. June 29, 2007, *available at* http://www.euractiv.com/en/security/eu-us-data-sharing-deals-renew-privacy-concerns/article-165077 (comments by MEP Sophie in't Veld, D66 Netherlands).

[98] 2007 Agreement, *supra* note 82, at 5.

[99] Ellen Nakashima, *E.U. Seeks Data on American Passengers*, THE WASHINGTON POST, Nov. 4, 2007, A18, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2007/11/03/AR2007110300956.html.

[100] *Id.*

domestically . . . That is exactly what they are talking about [in the proposed reciprocity plan]."[101] Thus, even while the 2007 Agreement did allay some European concerns—primarily by extending Privacy Act protections to non-U.S. citizens—concerns about the use of PNR data continue in both Europe and the United States.[102]

I. AUTOMATED TARGETING SYSTEM'S SYSTEM OF RECORDS NOTICE

In August 2007, soon after the conclusion of the 2007 Agreement, the Department of Homeland Security released a System of Records Notice ("SORN") for the new Automated Targeting System ("ATS"), used to implement the 2007 Agreement and screen PNR data received from Europe pursuant to that agreement.[103] As a screening tool, "ATS allows DHS officers charged with enforcing U.S. law and preventing terrorism and other crimes to effectively and efficiently manage information collected when travelers or goods seek to enter, exit, or transit through the United States."[104] ATS is the system in which CBP maintains information about travelers entering the United States; this system allows CBP "to determine whether a variety of potential risk indicators exist for travelers and/or their itineraries that may warrant additional scrutiny."[105] Thus, ATS provides the mechanism by which the PNR data is analyzed and stored by DHS and CBP. It is ATS, then, that is the subject of data request by both U.S. and European Citizens wishing to access and correct PNR data. The SORN notes that ATS is subject to the legal requirements of the Privacy Act and, as such, "[n]otwithstanding the listed exemptions for the system, individuals, regardless of their citizenship, may make a written request to review and access personal data . . . that is collected by CBP and contained in the PNR database stored in the ATS."[106] The ATS SORN, then, is another explanatory document; it alerts EU and U.S. citizens to rights

---

[101] *Id.* Identity Project is a privacy organization that focuses on the First Amendment implications of domestic data processing. *See* http://www.papersplease.org/who.html.

[102] *Id.*

[103] Automated Targeting System (ATS) System of Records Notice, 72 Fed. Reg. 43, 650 (Aug. 6, 2007).

[104] *Id.*

[105] *Id.*

[106] *Id.*

under the 2007 Agreement and further describes the processes and procedures for handling of PNR data.

IV. LOOKING FORWARD: REMAINING ISSUES IN PNR AGREEMENT NEGOTIATIONS

A. DEPARTMENT OF HOMELAND SECURITY 2008 REPORT

In December 2008, pursuant to a provision in the 2007 Agreement requiring periodical review of the implementation of PNR data exchanges, the U.S. DHS Privacy Office released "A Report Concerning Passenger Name Record Information Derived from Flights Between the U.S. and the European Union" ("2008 Report").[107] This report analyzed U.S. compliance with both the 2007 Agreement as well as the ATS SORN—noting those areas where the DHS and CBP were in compliance with the mandates of those documents and areas where improvements could be made.

Of particular importance were those areas where the Privacy Office found room for improvement—areas where DHS and CBP could bring themselves more in line with the requirements of the 2007 Agreement and ATS SORN. First, the 2008 Report noted that "if an individual requests 'all information held by CBP' the FOIA specialist generally does not search ATS because PNR was not specifically requested."[108] This is noteworthy because it suggests inadequate compliance with provisions of access and redress in the 2007 Agreement. Second, the 2008 Report notes that Privacy Act and FOIA personnel need to ensure that "where a PNR is indexed and retrieved by the requester's name or personal identifier and the information contains information pertaining to a third person whose information does not directly pertain to the individual requesting the information, the requestor only receives personally identifiable information about themselves."[109] To release a third party's information to the requestor

---

[107] Privacy Office, U.S. Department of Homeland Security, *A Report Concerning Passenger name Record Information Derived from Flights Between the U.S. and the European Union*, Dec. 18, 2008. (2008 Report), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pnr_report_20081218.pdf.

[108] *Id.* at 26.

[109] *Id.*

would be counter to the ATS SORN policy and provisions of the Privacy Act.[110]

In light of these two realizations about the handling of PNR data, the 2008 Report suggests that, with improved training of FOIA personnel, improvements can be made which will "improve response time, improve the quality of responses and the redaction, and the sufficiency of searches."[111]

However, even though the Privacy Office concluded that DHS and CBP are in compliance with the mandates of the ATS SORN and the 2007 Agreement, following the release of the 2008 Report, there was a flurry of media attention thrown on the issue—much of it critical of DHS handling of PNR data.

Of particular concern was the length of time it took DHS to answer requests for PNR data—typically more than one year and occasionally "many times longer than the legal time limits in the Privacy Act and Freedom of Information Act."[112] This is significant because, if requests are exceeding the time allowed under U.S. law, then not only are the rights of European citizens being violated, but also those of U.S. citizens.[113]

In response to criticisms of following the release of the 2008 Report, Hugo Teufel, Chief Privacy Officer at the Department of Homeland Security, released a statement emphasizing the legality of DHS and CBP under the 2007 Agreement and continued compliance with all federal and international obligations.[114] As to recommendations for improvement made in the 2008 Report, Teufel stated:

> [F]or every recommendation made in the report, there was a concrete and actionable response that CBP began to implement before the report was even issued. As

---

[110] *Id.*

[111] *Id.*

[112] *DHS Admits Problems in Disclosing Travel Surveillance Records*, PAPERS, PLEASE!, http://www.papersplease.org/wp/2008/12/24/dhs-admits-problems-in-disclosing-travel-surveillance-records/ (Dec. 24, 2008, 10:08 EST).

[113] *Id.*

[114] Posting of DHS, *What the Passenger Name Record Report Really Says*, LEADERSHIP JOURNAL ARCHIVE, http://www.dhs.gov/journal/leadership/2008/12/what-passenger-name-record-report.html (Dec. 31, 2008, 15:09 EST).

> with any program, improvements can always be made and so is the case here. CBP did not fail in meeting its commitments to the [2007] Agreement and Letters between DHS and the Council of the European Union. CBP actively contributed to the review, opening itself up to criticism while still trying to operationally meet the requirements of the 2007 Agreement and Letters.[115]

This statement is important because it emphasizes a continued need for improvement in how requests for PNR data are handled, while still acknowledging and reassuring citizens that proper privacy considerations and obligations are being met.

V. CONCLUSION

The questions that remain about the future of PNR Agreements between the U.S. and EU depend largely on the attitude of President Obama and the degree to which his attitude towards these agreements differs from that of his predecessor, President George W. Bush. While Europe generally views the new president's stance on foreign policy positively—especially his inauguration promises to end the "War on Terror" and restore compliance with international humanitarian law[116]—Europeans are not overly optimistic with regard to changes in the handling of PNR data.[117] In particular, one news source notes that although some sections of the U.S. government have shown renewed commitment to international agreements, "there has been no major initiative yet" from the Department of Homeland Security to "soften up on requirements," even though Secretary Janet Napolitano has shown a "difference of style" from the Bush Administration.[118]

If, even in the face of continued terrorist threats and plots around the world, the United States can show a renewed commitment to

---

[115] *Id.*

[116] *Europe Cheers as Obama Ends Bush's 'War on Terror*, EURACTIV.COM, Jan. 23, 2008, *available at* http://www.euractiv.com/en/priorities/europe-cheers-obama-ends-bush-war-terror/article-178757.

[117] Brian Beary, *Obama Gets Mixed Review from EU Data Protection Supervisor*, EUROPOLITICS, Nov. 19, 2009, *available at* http://www.europolitics.info/external-policies/obama-gets-mixed-review-from-eu-data-protection-supervisor-art255051-44.html.

[118] *Id.*

treaty obligations and compliance with international law, these efforts may go a long way in assuaging European concerns over privacy matters and will pave the way for the continuance of PNR Agreements.